

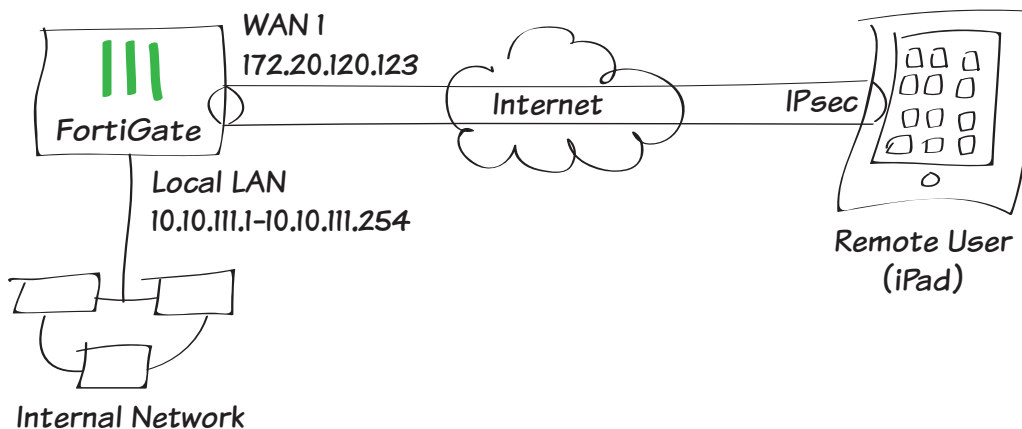
Configuring an IPsec VPN for iOS devices

This recipe uses the IPsec VPN Wizard to provide a group of remote iOS users with secure, encrypted access to the corporate network. The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet.



This recipe was tested using an iPad 2 running iOS version 7.1.

1. Creating a user group for iOS users
2. Adding a firewall address for the local network
3. Configuring IPsec VPN using the IPsec VPN Wizard
4. Creating a security policy for access to the Internet
5. Configuring VPN on the iOS device
6. Results

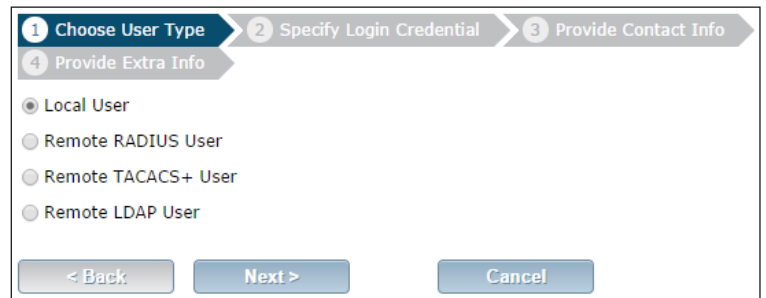


1. Creating a user group for iOS users

Go to **User & Device > User > User Definition.**

Create a new **Local User** with the User Creation Wizard.

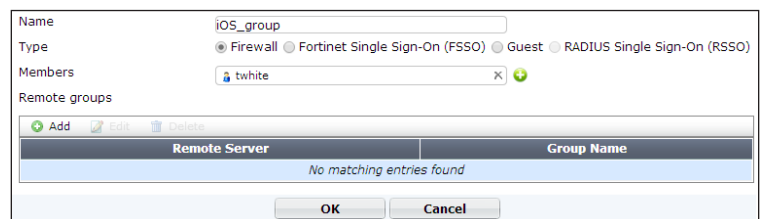
Proceed through each step of the wizard, carefully entering the appropriate information.



The screenshot shows the first step of the User Creation Wizard. At the top, there are four numbered steps: 1. Choose User Type, 2. Specify Login Credential, 3. Provide Contact Info, and 4. Provide Extra Info. Step 1 is currently active. Below the steps, there are four radio button options: **Local User** (selected), Remote RADIUS User, Remote TACACS+ User, and Remote LDAP User. At the bottom, there are three buttons: < Back, Next >, and Cancel.

Go to **User & Device > User > User Groups.**

Create a user group for iOS users and add the user you created.

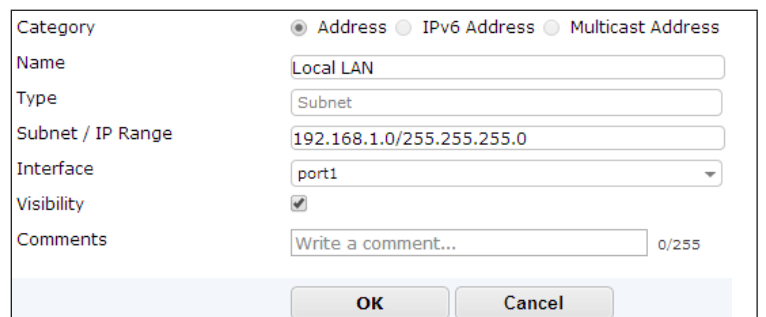


The screenshot shows the User Groups configuration page. The Name field is set to 'iOS_group'. The Type field has four radio button options: **Firewall** (selected), Fortinet Single Sign-On (FSSO), Guest, and RADIUS Single Sign-On (RSSO). The Members field contains 'twhite' with a search icon and a green plus icon. Below the Members field is a section for Remote groups with buttons for Add, Edit, and Delete. A table with two columns, Remote Server and Group Name, is shown with the message 'No matching entries found'. At the bottom, there are OK and Cancel buttons.

2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses.**

Add a firewall address for the Local LAN, including the subnet and local interface.

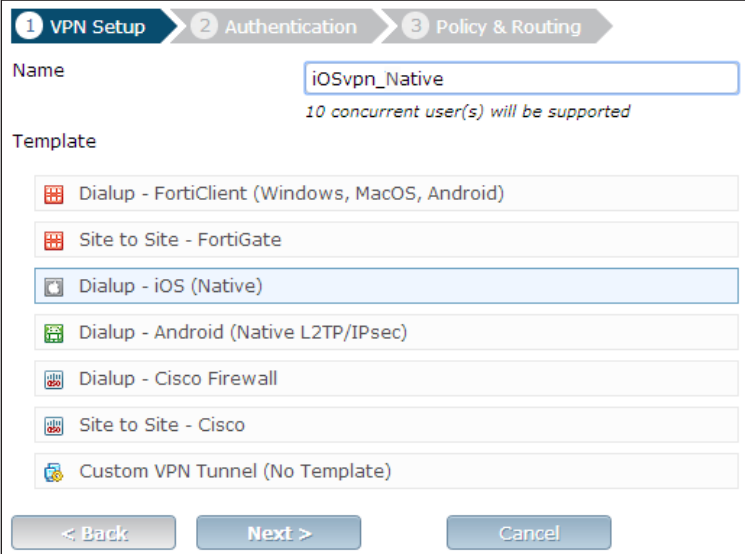


The screenshot shows the Address configuration page. The Category field has three radio button options: **Address** (selected), IPv6 Address, and Multicast Address. The Name field is set to 'Local LAN'. The Type field is set to 'Subnet'. The Subnet / IP Range field is set to '192.168.1.0/255.255.255.0'. The Interface field is set to 'port1'. The Visibility field is checked. The Comments field is set to 'Write a comment...'. At the bottom, there are OK and Cancel buttons.

3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPsec > Wizard**.

Name the VPN connection and select **Dial Up - iOS (Native)** and click **Next**.



The screenshot shows the first step of the IPsec VPN Wizard, 'VPN Setup'. At the top, there are three tabs: '1 VPN Setup' (active), '2 Authentication', and '3 Policy & Routing'. Below the tabs, the 'Name' field is set to 'iOSvpn_Native' with a note below it stating '10 concurrent user(s) will be supported'. Under the 'Template' section, a list of templates is shown: 'Dialup - FortiClient (Windows, MacOS, Android)', 'Site to Site - FortiGate', 'Dialup - iOS (Native)' (which is selected and highlighted in blue), 'Dialup - Android (Native L2TP/IPsec)', 'Dialup - Cisco Firewall', 'Site to Site - Cisco', and 'Custom VPN Tunnel (No Template)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

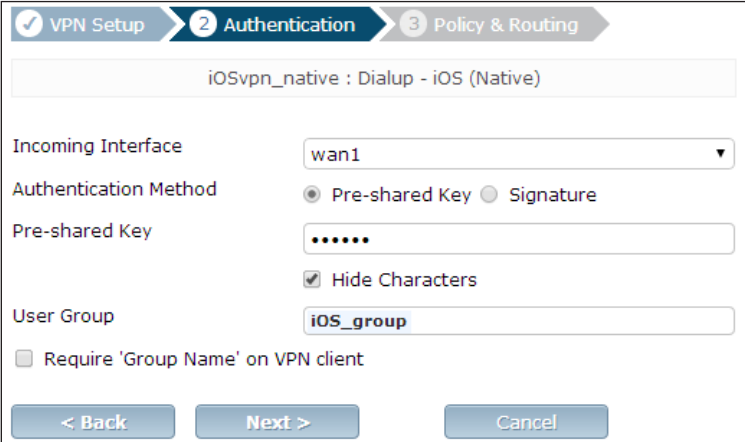
Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the iOS user group, then click **Next**.



The pre-shared key is a credential for the VPN and should differ from the user's password.



The screenshot shows the second step of the IPsec VPN Wizard, 'Authentication'. The tabs at the top are '1 VPN Setup', '2 Authentication' (active), and '3 Policy & Routing'. The title bar at the top reads 'iOSvpn_native : Dialup - iOS (Native)'. Below this, the 'Incoming Interface' is set to 'wan1' in a dropdown menu. The 'Authentication Method' is set to 'Pre-shared Key' with a radio button, and 'Signature' is unselected. The 'Pre-shared Key' field contains seven dots, and the 'Hide Characters' checkbox is checked. The 'User Group' is set to 'iOS_group' in a dropdown menu. At the bottom, there is an unchecked checkbox labeled 'Require 'Group Name' on VPN client'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the local LAN address.

Enter an IP range for VPN users in the **Client Address Range** field.



The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the **_range** suffix (in this case, **iOSvpn_Native_range**).

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.

The screenshot shows the 'Policy & Routing' step of the 'iOSIPsecVPN : Dialup - iOS (Native)' configuration. The 'Local Interface' is set to 'port1', 'Local Address' is 'Local LAN', 'Client Address Range' is '10.10.111.1-10.10.111.254', and 'Subnet Mask' is '255.255.255.255'. Under 'DNS Server', 'Use System DNS' is selected. The 'Enable IPv4 Split Tunnel' checkbox is unchecked. At the bottom are buttons for '< Back', 'Create', and 'Cancel'.

4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote iOS users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **all** and ensure that you enable **NAT**.

The screenshot shows the 'Policy' configuration page for IPv4. The 'Incoming Interface' is 'iOSvpn_Native', 'Source Address' is 'all', 'Source User(s)' is 'Click to add...', 'Source Device Type' is 'Click to add...', 'Outgoing Interface' is 'wan1', 'Destination Address' is 'all', 'Schedule' is 'always', 'Service' is 'ALL', and 'Action' is 'ACCEPT'. Under 'Firewall / Network Options', 'NAT' is turned ON, and 'Use Destination Interface Address' is selected.


5. Configuring VPN on the iOS device

On the iPad, go to **Settings > General > VPN** and select **Add VPN Configuration**.

Enter the VPN address, user account, and password in their relevant fields. Enter the pre-shared key in the **Secret** field.

CancelIPsec VPN 5.2Save

L2TPPPTPIPsec



DescriptionIPsec VPN 5.2

Server172.20.120.123

Accounttwhite

Password•••••

Use Certificate☐

Group Name

Secret•••••

PROXY

OffManualAuto

6. Results

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and view the status of the tunnel.

Name	Type	Remote Gateway	Username	Status	Incoming Data
iOSvpn_Native_0	Dialup	172.20.120.16		Up	9.22 K

Users on the internal network will be accessible using the iOS device.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

RefreshDownload Raw Log

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
4	11:21:42	port1		192.168.1.117	208.91.113.70	304 B / 304 B

Select an entry to view more information.

Dst	192.168.1.114	Virtual Domain	root
Received	72	Source Country	Reserved
Sent / Received	72 B / 72 B	Duration	63
Sent	72	Application Details	
Service	PING	Protocol	1
Destination Country	Reserved	roll	65428
Status	✓	Timestamp	Thu Feb 21 11:20:44 2014
Tran Display	noop	Sequence Number	220067
Policy ID	6	Src Interface	iOSvpn
Src	10.10.111.16	VPN	iOSvpn_Native
Sent Packets	2	Level	notice
VPN Type	ipsec-dynamic	logid	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	11:20:44 (Thu Feb 21 11:20:44 2014)
Dst Interface	port1		

Remote iOS users can also access the Internet securely via the FortiGate unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Select an entry to view more information.

Refresh Download Raw Log						
#	Y Date/Time	Y Src Interface	Y Dst Interface	Y Src	Y Dst	Y Sent / Received
1	11:28:43	ios_P1	wan1	10.10.111.16	74.121.50.17	1023 B / 579 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
4	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
5	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.105	812 B / 642 B
6	11:20:42	iOSvpn_Native	wan1	10.10.111.16	74.125.134.102	808 B / 712 B
7	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.94	2.96 KB / 23.07 KB
8	11:20:35	iOSvpn_Native	wan1	10.10.111.16	17.149.36.134	104 B / 60 B
9	11:19:15	iOSvpn_Native	wan1	10.10.111.16	204.93.33.67	813 B / 365 B

Dst	74.121.50.17	Virtual Domain	root
Received	579	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	1023 B / 579 B
Duration	2	Sent	1023
Src NAT Port	50189	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65428	Status	close
Timestamp	Thu Feb 21 11:28:43 2014	Tran Display	snat
Sequence Number	221594	Policy ID	7
Src Interface	iOSvpn_Native	Src	10.10.111.16
VPN	iOSvpn	Sent Packets	6
Level	notice	VPN Type	ipsec-dynamic
Src Port	50189	logid	13
Sub Type	forward	Threat	
Received Packets	4	Date/Time	11:28:43 (Thu Feb 21 11:28:43 2014)
Dst Interface	wan1		

You can also view the status of the tunnel on the iOS device itself.

On the device, go to **Settings > VPN > Status** and view the status of the connection.

Lastly, using a Ping tool, you can send a ping packet from the iOS device directly to an IP address on the LAN behind the FortiGate unit to verify the connection through the VPN tunnel.

Server172.20.120.123

Connect Time9:48

Connected to172.20.120.82

IP Address10.10.111.1

IP Address to ping:

StartClear

8.8.8.8

Delay: 2000 ms

Result:

PING 172.20.120.123 (172.20.120.123)
36 bytes from 172.20.120.123 : icmp_seq=0 ttl=254 time=12 ms
36 bytes from 172.20.120.123 : icmp_seq=1 ttl=254 time=5 ms
36 bytes from 172.20.120.123 : icmp_seq=2 ttl=254 time=10 ms
36 bytes from 172.20.120.123 : icmp_seq=3 ttl=254 time=10 ms
--- 172.20.120.123 ping statistics ---
4 packets transmitted, 4 packets received, lost 0.0 %